

UNITED STATES DISTRICT COURT
for the
District of Delaware

In the Matter of the Search of }
 (Briefly describe the property to be searched }
 or identify the person by name and address) }
 INFORMATION ASSOCIATED WITH CERTAIN ACCOUNTS }
 THAT ARE STORED AT PREMISES CONTROLLED BY }
 GOOGLE LLC AND GOOGLE PAYMENT CORPORATION }
) Case No. 23-439M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A.

located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC § 1591, 2421-2424, 1589	Sex trafficking, Mann Act, Forced Labor

The application is based on these facts:

See attached Affidavit.

Continued on the attached sheet.

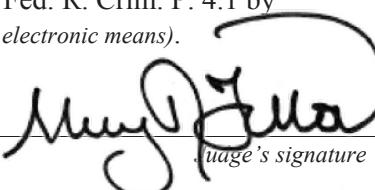
Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Kason Washington

Applicant's signature

Kason Washington, Special Agent, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____
telephone _____ (*specify reliable electronic means*). 

Date: October 13, 2023

City and state: Wilmington, DE

Hon. Sherry R. Fallon, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
CERTAIN ACCOUNTS THAT ARE
STORED AT PREMISES CONTROLLED
BY GOOGLE LLC AND GOOGLE
PAYMENT CORPORATION

Case No. 23-

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

I, Kason Washington, a Special Agent (“SA”) of the United States Department of Homeland Security, Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), Eastern Shore (“HSI Eastern Shore”), Maryland Office, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts, hereinafter the “SUBJECT ACCOUNTS,” that are stored at premises controlled by Google LLC and Google Payment Corporation (“Google”), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The SUBJECT ACCOUNTS are as follows:

- a. **bwaters420@gmail.com**
- b. **brookewaters@gmail.com.**

2. The information to be searched is further described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC and Google

Payment Corporation (“Google”) to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent authorized to investigate violations of laws of the United States and execute warrants issued under the authority of the United States. I have been employed by ICE/HSI since February 2021. My initial training with HSI consisted of attending and graduating from the Basic Criminal Investigators Training Program and the Homeland Security Investigation Special Agent Training Program of instruction which is conducted at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. Pertinent to this affidavit and prior to my employment with ICE/HSI, beginning in 2016, I held the position of Police Officer with the Cambridge, Maryland Police Department. During my tenure with the Cambridge Police Department (CPD), I served in positions to include Patrolman, Detective, Community Police Officer, and Emergency Response Team (ERT) team member. While working at the CPD, I investigated and participated in the investigations of matters involving homicides, bank robberies, fraud, narcotics, and sexual assaults. As part of my daily duties as an HSI agent, I have conducted, participated in, and/or received training in numerous investigations of criminal activity, including, but not limited to, the investigation of narcotics offenses, money laundering, fraud, human trafficking, child exploitation and child pornography, alien smuggling, human trafficking, and Title III wire communication interception investigations. I have gained experience through training at the FLETC and through everyday work, as assigned and via assisting other law

enforcement officers, relating to the aforementioned types of investigations. Pertinent to this investigation, in September 2023, I obtained advanced training related to human trafficking via the International Association of Human Trafficking Investigators (IAHTI) – Annual Human Trafficking Conference.

4. As such, I am a federal law enforcement officer engaged in the enforcement of federal criminal laws, including the SPECIFIED FEDERAL OFFENSES listed below. I am authorized by the Secretary of the Department of Homeland Security to request the issuance of search warrants.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. The information contained in this affidavit is based, in part, on my first-hand knowledge, information I have reviewed, as well as information given and explained to me by other law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have not, however, knowingly withheld any fact necessary to a determination of probable cause.

6. The government is seeking updated warrants for the SUBJECT ACCOUNTS. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the below-specified federal statutes have been committed by Brooke WATERS (“WATERS”) and co-defendant Clifton GIBBS (“GIBBS”), and that evidence of said violations will be contained in the SUBJECT ACCOUNTS past the date of the last search warrants, namely past 2019. There is also probable cause to search the information described in Attachment A, and for evidence of these crimes, as described in Attachment B.

SPECIFIED FEDERAL OFFENSES

7. The investigation concerns alleged violations of the SPECIFIED FEDERAL OFFENSES, which include: Title 18 U.S.C. § 1591 (Sex Trafficking); Title 18 U.S.C. §§ 2421-2424 (the Mann Act); and Title 18 U.S.C. § 1589 (Forced Labor).

- a. In pertinent part, Title 18 U.S.C. § 1591 (Sex Trafficking) prohibits any person from knowingly, (1) in or affecting interstate commerce, recruiting, enticing, harboring, transporting, providing, obtaining, maintaining, patronizing, or soliciting by any means a person; or (2) benefitting financially or receiving anything of value from participation in a venture which has engaged in an act described in violation of (1) above, knowing, or in reckless disregard of the fact, that force, fraud, and coercion, or any combination of such means, would be used to cause the person to engage in commercial sex acts.
 - i. Per 18 U.S.C. § 1591(e)(2), “coercion” means (a) threats of serious harm to or physical restraint against any person; (b) any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or (c) the abuse or threatened abuse of law or the legal process.
 - ii. Per 18 U.S.C. § 1591(e)(3), “commercial sex act” means any sex act on account of which anything of value is given to or received by any person.
- b. In pertinent part, Title 18 U.S.C. §§ 2421-2424 (the Mann Act) prohibits any person from knowingly transporting a person in interstate commerce with the intent that the person engage in prostitution or any sexual activity for which any person may be charged with a criminal offense.
- c. In pertinent part, Title 18 U.S.C. § 1589 (Forced Labor) prohibits any person from knowingly providing or obtaining the labor or services of a person by means of force, threats of force, physical restraint, or threats of physical restraint to that person or another; by means of serious harm or threats of serious harm to that person or another; by means of the abuse or threatened abuse of law or legal process; or by means of a scheme, plan, or pattern intended to cause the person to believe that, if she did not perform such labor or services, she would suffer serious harm or physical restraint.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is “a court of

competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND ON SEX TRAFFICKING/DEFINITIONS

9. Through my investigations, training, and experience, and working with other law enforcement officers experienced in human trafficking investigations, I have learned that individuals who engage in the sex and labor trafficking of others target individuals who are particularly vulnerable, such as drug addicts, and often use violence, drugs and drug addiction, alcohol, threats, and manipulation to maintain control over the individuals they cause (through fraud, force, or coercion) to engage in commercial sex or forced labor. Additionally, traffickers use fraud such as romance schemes to defraud or coerce their victims. In both types of trafficking, physical violence and threats, manipulation of drug addiction, coupled with intermittent acts of kindness, are often used to increase the victims’ emotional and physical dependence on the traffickers. The traffickers also generally have rules and forms of discipline that they typically use to maintain order and compliance over their victims.

10. The term “date” refers to an instance of commercial sex. The term “date” also may refer to a person, commonly referred to as a “John”, who buys commercial sex.

11. The term “bottom” or “bottom bitch” typically refers to a woman designated by the trafficker to supervise or control the other victims and/or help manage the sex trafficking business. The “bottom” often acts as an enforcer and the trafficker’s right-hand person, performing such duties as instructing victims on how to post commercial sex advertisements, posting such

advertisements, collecting money, booking hotel rooms, punishing the victims for disobeying rules, or reporting disobedience to the trafficker.

12. Backpage.com was a commercial advertising website used to buy and sell items. Backpage.com also had an adult section commonly seen by law enforcement to contain ads soliciting commercial sex for money and was commonly used by sex traffickers to advertise victims for commercial sex. In order to post an advertisement on Backpage.com, the user established an account by providing an email address and password. The email address became that particular account's username. In April 2018, the Department of Justice took down and seized Backpage.com. As such, Backpage.com is no longer active. But the Federal Bureau of Investigation has possession of Backpage.com's servers and, as a result, ads posted on Backpage.com.

13. "Incalls" are when a hotel room or other venue is secured by a trafficker, pimp, or prostitute for the purposes of performing commercial sex acts. "Outcalls" are when an individual performing commercial sex acts travels to a location where a "John" is already located.

14. The term "dope sick" is used to describe opiate withdrawal symptoms such as the symptoms an addict experiences when the addict has not used heroin for a period of time or has used less heroin than usual. The physical side effects are intensely uncomfortable and include nausea, vomiting, insomnia, body aches, and diarrhea. Addicts often continue to use drugs solely to avoid becoming dope sick.

PROBABLE CAUSE

Background of Investigation

15. On April 13, 2023, a Grand Jury for the District of Delaware returned a seventeen-count indictment against the Defendants, charging them with committing, and aiding and abetting each other to commit, nine counts of sex trafficking, six counts of labor trafficking, and one count each of the Mann Act. The indictment alleges crimes against 13 victims, referred to in the indictment as Victims 1 through 13. The victims will be referred to in the same manner herein. On April 13, 2023, the United States District Court for the District of Delaware issued warrants for the Defendants' arrests, and those arrests were executed on May 10, 2023. Following his arrest, GIBBS waived *Miranda* and participated in a voluntary interview conducted by HSI.

16. The federal investigation of the Defendants began in February 2015, when local law enforcement arrested GIBBS and WATERS, along with Victims 5 and 6, in two separate incidents in Ocean City, Maryland. Law enforcement initiated a traffic stop of GIBBS' vehicle. Upon a consent search of Victim 5's purse and subsequent search of the vehicle (registered to GIBBS), law enforcement located heroin, cocaine, and drug paraphernalia. As a result, GIBBS was charged with possession of cocaine. Separately, law enforcement encountered WATERS and Victim 6 in another vehicle outside of a Quality Inn hotel and conducted a welfare check on WATERS, who appeared to be under the effects of narcotics. Law enforcement discovered 11 bags of heroin on WATERS' person and charged her with possession of heroin.

17. It was later determined that GIBBS and WATERS had posted advertisements for dates with Victims 5 and 6 on Backpage.com and transported them to Maryland for the purpose of

commercial sex.¹ HSI Special Agents and Ocean City Police Department officers interviewed Victims 5 and 6, as well as GIBBS after he waived *Miranda*. When he was shown Backpage.com advertisements of Victim 5 and Victim 6, GIBBS admitted that the photos appeared to be taken inside his home in Lewes, DE, but claimed that he did not know who took the photos and denied any involvement in prostitution activities. WATERS also waived *Miranda*, but was experiencing withdrawal symptoms and could not be interviewed. Victims 5 and 6 informed law enforcement that they were engaging in commercial sex to repay GIBBS and WATERS for illicit drugs and housing.

18. In March, May, and July 2022, while represented by counsel, WATERS sat voluntarily for three interviews with HSI agents and federal prosecutors. WATERS explained that she had been in an episodic romantic relationship with GIBBS for over ten years and acknowledged that she served as his “bottom ho” for his commercial sex business.

19. The investigation showed that soon after Victims 1 through 13 arrived at one of the properties used by the Defendants, GIBBS used his knowledge of the Victims’ living situations, finances, and drug addictions—and their fear of painful withdrawal symptoms—to exploit their vulnerabilities and to create an atmosphere in which Victims had to pay for the expenses they incurred, or would obtain thereby establishing a “debt,” and to pay for future drugs which GIBBS and WATERS knew the Victims would need to avoid withdrawal sickness, as well as ongoing housing provided. While at the isolated and/or rural locations, the Defendants controlled the Victims’ access to drugs (they would not permit the Victims to buy drugs from anyone else

¹ This conduct is captured in Count 16 of the indictment.

while they were working for and/or living with GIBBS) and used the Victims' inevitable dope-sickness and fear of dope-sickness, among other tactics, to coerce them to engage in commercial sex acts, boosting, panhandling, and other forms of labor, providing childcare for GIBBS' minor child, and burning trash and performing manual labor on all the properties.

20. After doing dates, boosting, or performing other money-making activities, the Defendants required the Victims to turn over the money, often cash, they made before supplying them with additional narcotics. For both sex and labor trafficking victims, WATERS purported to keep track of how much money the Victims owed, and some Victims kept track of how much money they generated in relation to the amount of drugs supplied to them. Victim statements often indicated that the amount of drugs provided was not equal to the amount of revenue generated. During her interview in March 2022, WATERS stated that GIBBS would ask her about how much money the "girls" were making on dates. WATERS also stated GIBBS did not want information about their criminal activity "on paper" but that she tried to write things down in code for several days. WATERS stated that GIBBS would keep track of the "girls" and how much they were bringing in, but did not explain how. She said that she would keep track of the funds the best she could.

21. In furtherance of their trafficking scheme, GIBBS and WATERS took photos of the Victims, which they used for commercial sex advertisements, and arranged numerous commercial sex dates through electronic means. Financial records and witness statements corroborate that the Defendants also purchased lingerie (which GIBBS called a "work uniform"), paid for advertisements (including by using gift cards and/or pre-paid cards), paid for hotel rooms at multiple hotels, and transported and/or arranged the transportation of the Victims to their "dates,"

including in vehicles controlled by the Defendants. They provided the Victims with cell phones and instructed them on how and when to use them during dates, and set the rates for engaging in commercial sex acts with the Victims. Statements from victims and witnesses show that hourly rates often ranged from \$100 to \$300. Victims and witnesses told law enforcement that they made substantial amounts of money performing multiple dates per day, all of which they handed over to the Defendants. For example, Victim 5 relayed that she had attempted to track her earnings for a three-week period by writing them on a notebook she hid under a mattress; she estimated that she made \$29,980 during that time and said all of it went to the Defendants.

22. With respect to the forced labor victims, WATERS told the government that in the summer of 2017, she and other known individuals and Victims, began boosting items, like power tools and baby items. GIBBS and WATERS provided lists of items to steal and the Victims would go and steal, or “boost,” the items, often from local outlet stores or home improvement stores, and would then drive the Victims to the stores. Such lists, including some with photographs of specific items to steal, were found in WATERS’ Facebook account. WATERS often transported the Victims to the boosting locations and back to GIBBS’ properties. The Victims turned the items over to the Defendants, who then personally used the items or resold them, as shown in WATERS’ Facebook Marketplace and Craigslist accounts.

23. WATERS ultimately decided to cease meeting with the government and went back to live with GIBBS later in 2022 and was living him at the time they were arrested in May 2023.

24. At the time of arrest, law enforcement executed search warrants for GIBBS and

WATERS' premises.² Pursuant to the search warrants, multiple devices were seized and subsequently searched.

Use of the SUBJECT ACCOUNTS in Criminal Activity

25. The SUBJECT ACCOUNTS are two Gmail accounts associated with WATERS. As described in more detail below, WATERS has utilized Google accounts, including the SUBJECT ACCOUNTS, in conjunction with Backpage, Craigslist, and Facebook, to effectuate the charged criminal conduct since 2014. Furthermore, a review of legal process from Backpage.com, GIBBS' AOL account, and the 2019 returns of WATERS' Gmail accounts (including the SUBJECT ACCOUNTS) shows that WATERS used her Gmail accounts to communicate with GIBBS in furtherance of the SPECIFIED FEDERAL OFFENSES.

26. The 2019 warrant returns from Google included the content of six Gmail accounts associated with WATERS, including the two SUBJECT ACCOUNTS.³ These returns, plus records obtained from Backpage.com, show that WATERS, aided and abetted by GIBBS, used at least four Gmail addresses to post a total of 909 advertisements for commercial sex related to Victims 1 through 7—and other women—from April 2014 through November 2016. In those 909 advertisements, WATERS listed 33 unique phone numbers as the contact numbers. Additionally, the returns contain confirmation emails in 2014 and 2015 from hotels (*e.g.*, Sleep

² Search Warrants 23-200M, 23-201M, 23-202M, and 22-203M, signed by the Honorable Jennifer L. Hall, U.S. Magistrate Judge.

³ Search Warrant Nos. 19-56M and 19-147M, signed by the Honorable Sherry R. Fallon, U.S. Magistrate Judge.

Inn Rehoboth Beach, and Rodeway Inn and Suites) known to be used in furtherance of the commercial sex operation she ran with GIBBS.

27. The 2019 returns also showed that the SUBJECT ACCOUNTS received many emails sent in response to commercial sex ads placed on Craigslist and other unspecified dating sites. It appears that WATERS stopped using four of the six accounts to send or receive information related to commercial sex in 2015 or 2016. It appears, however, that she continued using the two SUBJECT ACCOUNTS for commercial sex postings much closer in time to the execution of the search warrants in 2019. For instance, in February 2019, WATERS received an email at the brookewaters@gmail.com account in response to an ad she placed on an unnamed site. Additionally, WATERS received two emails sent to her bwaters420@gmail.com in late 2018 and early 2019 confirming that she had set-up profiles on other commercial sex/dating sites such as “3Fun dating app,” “DateHookup,” “SeekingArrangement,” and “The Erotic Review.”

28. WATERS also sent emails to GIBBS that corroborate the use of drugs in their coercive scheme. For instance, in 2014, WATERS forwarded an email to GIBBS about whether addiction is a disease or a choice. In another email from 2014, WATERS references a fight she had with Victim 4 in which Victim 4 said that GIBBS respected her and the other “hoes” because they make money for GIBBS, and since WATERS does not make money, GIBBS does not respect her. WATERS went on to say that she did not know how “to deal with the way u [GIBBS] interact with them [Victims] I got hooked on drugs.” WATERS then wrote that GIBBS treated the Victims with affection because “they send u money or give u money and money makes you so happy.”

29. The evidence gathered in the accounts further indicates that WATERS and other

individuals began boosting in 2017. The 2019 returns show that WATERS' bwaters420@gmail.com account contained multiple photos of items, like power tools and outdoor equipment, consistent with the types of items WATERS conceded she and other Victims would boost for resale. Furthermore, WATERS used her Google Voice number to communicate with individuals interested in buying items she posted for sale. Between November 2017 and January 2018, WATERS used her Google Voice account to respond to individuals asking to purchase items, including a Roku device and a pressure washer. These items are similar in nature to the items WATERS posted for sale on Facebook Marketplace.

Evidence Found in Phones Searched and Seized

30. Following the execution of the arrest warrant, WATERS' two phones were seized and searched. The first phone is an Android and included a contact named "HomieLuvaFriend" associated with GIBBS' primary phone number. This phone shows that WATERS used the following Google suite of services associated with her name or Gmail account: Duo, Meet, Gmail, Google Phone, Account, and Google Photos. The phone also shows that WATERS used many of Google's services associated with two of GIBBS' Gmail accounts, including Google Photos, Accounts, and Google Drive on her phone. This phone also contains texts between WATERS and GIBBS which occurred around the time WATERS was meeting with the government. On May 19, 2022, a few days after her second meeting with the government, WATERS texted GIBBS saying "I sent u an email. Too much to text. Please read it." Soon after, GIBBS responded by saying "I just read it...I don't like you saying they got enough to do anything against me."

31. WATERS' second Android phone showed that she used the following Google suite of services associated with her name or Gmail account: Duo, Chrome, Gmail, Google Pay, Accounts, and Google Drive. The phone also showed that WATERS used many of Google's services associated with the same two of GIBBS' Gmail accounts, including Chrome, Accounts, and Google Drive. The phone also contains GIBBS as a contact and includes additional texts between WATERS and GIBBS. Specifically, on May 19, 2022, GIBBS texted "Ok so what truth has been revealed of me harming or threatening to harm anyone?" GIBBS then texted "I can't go to jail."

32. WATERS' phone also contains relevant texts with her adult daughter, Hannah, implicating the use of her e-mail accounts. In April and May 2022, the following exchange took place:

WATERS: I think cliff getting my emails and my venmo stuff is emailed and I'm trying to figure out how to get my emails off them phones he has still

Hannah: Sign out of all devices in settings

WATERS: I can't find that option in my Gmail settings...just sign out of device I'm on

Hannah: It's on there somewhere I've done it before with my Gmail. That or change your password and when you do it should give you an option to sign out of devices or stay logged in.

WATERS: Ok..let me try that. 1 of my emails was opened and I didn't open it and it was about my foodstamp application. I be looking at his emails all the time then mark them as UNREAD...I'mm thinking he or [Victim 4] doing same thing and forgot with this one.

WATERS: So somehow you can see my location at all times through your Google email acct

Hannah: Google sent me a notification

WATERS: Welp there u go. This is just in case I go missing. You also are the only email allowed to access my Google acct if it goes inactive.

33. At the time of seizure, both of WATERS' phones still contained numerous contact entries for "Hoe phones," several of which match numbers on Backpage ads posted by

WATERS. Additionally, both phones contain contact entries for hotels and motels (*e.g.*, Red Mill Inn, Heritage Inn, Rehoboth Inn) known to have been used for commercial sex dates.

Discussion of Email Usage on Jail Calls

34. Since she has been in pre-trial detention, WATERS has spoken about at least one of the SUBJECT ACCOUNTS on recorded jail calls and text messages indicating that evidence related to the charged criminal conduct could be found in her account.

35. In another call, WATERS told Hannah that Hannah had access to WATERS bwaters420@gmail.com account when WATERS “knew this was all going down”—believed to be a reference to the time after WATERS began meeting with the government. In a later call, WATERS identified the relevant account as bwaters420@gmail.com and provided Hannah with the password. Other evidence in the case establishes that Hannah has also spoken to GIBBS’ adult daughter, Courtney, about aspects of the charged conduct.

36. WATERS has also communicated with GIBBS’ adult daughter, Courtney, about topics including the charged conduct. In a message that Courtney appears to have forwarded from GIBBS to WATERS, GIBBS wrote to WATERS “take notes remembe times nd dates” and then said “tell her [WATERS] if i knew who each victim by number is it would help put times tes and things in perspective... also we need that contract that stated no sex for money that was posted on backpage.” WATERS replied “[g]et me the timeline and I will figure that out for us. Backpagw stuff is on email and Hannah has access to my email.”

Summary

37. In summary, the 2019 return of WATERS' Google accounts shows her consistent use of the SUBJECT ACCOUNTS to perpetuate the SPECIFIED FEDERAL OFFENSES—including using the accounts after she was aware of HSI's involvement in the case following her arrest in 2015. Additionally, WATERS' own statements to the government in 2022 combined with other evidence, such as the Facebook returns, led the government to indict her and GIBBS for conduct which occurred after 2019. Finally, information contained in WATERS' phone indicates that she was emailing with GIBBS about the charged conduct as recently as 2022. All of this establishes probable cause that additional evidence of the SPECIFIED FEDERAL OFFENSES exists in the SUBJECT ACCOUNTS post-May 2019, the last date on which the government obtained information from the SUBJECT ACCOUNTS.

BACKGROUND CONCERNING GOOGLE⁴

38. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service

⁴ The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at ers.google.com; product pages on support.google.com; or product pages on about.google.com.

called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

39. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

40. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

41. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

42. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

43. Google provides an address book for Google Accounts through Google Contacts.

Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

44. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

45. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user has not

disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

46. Google Drive is a cloud storage service automatically created for each Google account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

47. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.

48. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

49. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

50. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google

Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

51. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

52. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other

browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

53. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

54. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and

send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

55. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

56. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

57. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed),

the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

58. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

59. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For instance, if any individual searches for federal criminal statutes related to the conduct under investigation or for victims and witnesses associated with the investigation, this evidence could provide evidence of consciousness of guilt.

60. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic (*e.g.*, location information integrated into an image or video sent via email or chat) and chronological context of access, use, and events relating to the crime under investigation.

61. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

62. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. It might be the case that the targets downloaded bank and cash transfer applications which will reveal otherwise unknown money which might be the proceeds of criminal activity. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

63. Your affiant knows that the requested information includes information which

Google is able to provide that will assist law enforcement in identifying other accounts associated with the SUBJECT ACCOUNTS. This information includes any forwarding or fetching accounts relating to SUBJECT ACCOUNTS, all other Google accounts linked to the SUBJECT ACCOUNTS because they were accessed from the same computer, all other Google accounts that list the same SMS phone number as the SUBJECT ACCOUNTS, all other Google accounts that list the same recovery email address as does the SUBJECT ACCOUNTS, and all other Google accounts that share the same creation IP address as the SUBJECT ACCOUNTS. This information will assist law enforcement in identifying the users of the SUBJECT ACCOUNTS.

64. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

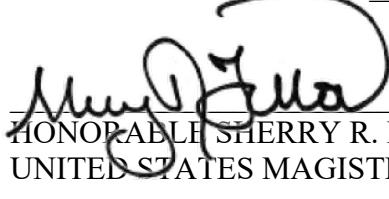
65. Based on the foregoing, I request that the Court issue the proposed search warrant.

66. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google LLC and Google Payment Corporation ("Google"). Because the warrant will be served on Google LLC and Google Payment Corporation ("Google"), who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Kason Washington
Kason Washington
Special Agent
Homeland Security Investigations

Sworn to me over the telephone and signed by me pursuant to
Fed. R. Crim. P. 4.1 on this 13th day of October, 2023:


HONORABLE SHERRY R. FALLON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the SUBJECT ACCOUNTS, listed below, that are stored at premises owned, maintained, controlled, or operated by Google LLC and Google Payment Corporation (“Google”), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043:

- bwaters420@gmail.com
- brookewaters@gmail.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by: Google LLC and Google Payment Corporation (“Google”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703. On August 9, 2023, all but one of the SUBJECT ACCOUNTS were preserved by Google via reference number 40064518. Google is required to disclose to the government for each account or identifier listed in Attachment A the following information for the time period May 9, 2019 to present, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the Account, including:
 1. Names (including subscriber names, user names, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
 3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
 5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
 6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and
8. Change history.

- b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs
- d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails. All forwarding or fetching accounts relating to the accounts;
- e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history
- f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
- h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, Android applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and

change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

- i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
- j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers;
- k. All Location History & Web App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;
- l. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history;
- m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;
- n. All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history;

- o. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

Google is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and/or instrumentalities of violations of SPECIFIED FEDERAL OFFENSES, those violations involving BROOKE WATERS and occurring after May 9, 2019, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Records and information relating to the SPECIFIED FEDERAL OFFENSES, to include, commercial sex acts, prostitution, interstate travel for purposes of commercial sex or prostitution, or promotion of commercial sex or prostitution, sex trafficking, forced labor trafficking, organized theft, use or sale of drugs;
- (b) Evidence indicating how and when the Account were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the Account about matters relating to the SPECIFIED FEDERAL OFFENSES, including records that help reveal their whereabouts.